REMARKS

Reconsideration of the application is respectfully requested for the following reasons:

1. Amendments to Claims

In the Advisory Action, the Examiner indicates that the claimed modification of radiated signals reads on Dunlavy's *masking* of radiated signals. It appears that the Examiner has overlooked or misunderstood the language in the original claims that refers to modification of radiated signals *by appropriate selection of commands or by modifying execution of commands so that detection of signals resulting from* ***execution*** *of commands does not betray the data processed by the program.* Therefore, the first two independent claims 1 and 22 have been revised so that the command execution feature can more readily be understood by the Examiner.

In addition, the claims have been amended to even more clearly specify that the purpose of the invention is to make it difficult to detect **signals generated *as a result of* execution of the operating program commands**, which the Examiner has confused with Candelore's **data transmissions** to and from an external memory.

2. Rejection of Claims 1-4, 13-25, and 34-41 Under 35 USC §103(a) in view of U.S. Patent No. 6,061,449 (Candelore) and 5,297,201 (Dunlavy)

This rejection has been maintained on the grounds that:

a. *The Examiner believes that changing the sequence of data retrieval from memory does constitute a modification of execution of commands to prevent the commands from being inferred*, and

b. *The Examiner further believes that Dunlavy's teaching of masking the radiated signals does read on the limitation of Claim 1, recited in the alternative, that the "operating program commands are executed by the data carrier in such a way that the data processed with the corresponding command cannot be inferred from the detected signals."*

In reply, the Applicant respectfully submits that:

a. Candelore actually teaches changing the *transmission* sequence of data retrieval from memory in a way that does not require modification for command execution, and

b. The claim language cited by the Examiner states that "*program commands **are executed** in such a way. . .*," wherein as Dunlavy is not concerned with program execution, but rather with masking of radiated signals irrespective of program execution.

The system and method of Candelore concerns the manner in which data is transmitted between an *external* memory and a processor. Instead of transmitting and storing the data sequentially, in the order that the data is used by a processor, the addresses and order in which the data is transmitted is scrambled. When the scrambled data is received by buffers connected to the processor, the data is re-ordered so that the processor can access the data in the required sequence.

The method of Candelore may be understood from the following simplified example:

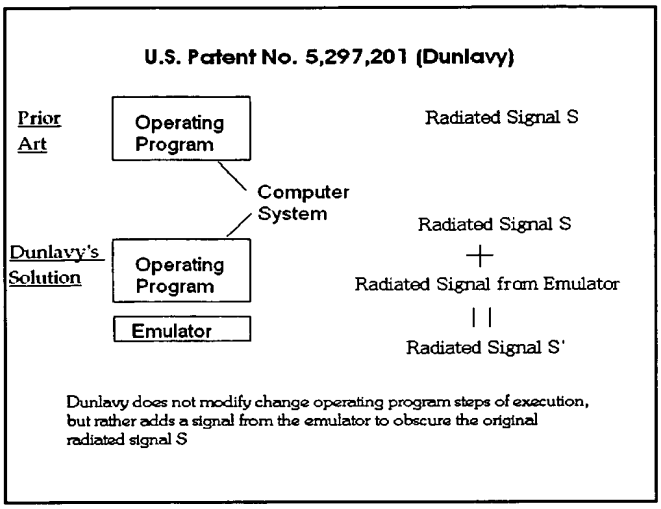
A program consists of the steps Get A, process A, Get B, Process B, Get C, and Process C. In a conventional method, A, B, and C would be transmitted from the external memory to the buffers in sequence. However, Candelore scrambles the transmission so that, for example, the order of transmission is C, B, A. When the data reaches the buffer, it is re-arranged or marked so that the processor can access the data in the sequence A, B, and C. As a result, the order of data cannot be discovered by intercepting the transmission, ***and yet execution of the program is <u>not</u> affected.*** This is clearly not the same as the claimed invention, which modifies the order of execution of the program (for example, Get B might precede Get A) or chooses steps (GetB' and GetA') that make it difficult to infer the data being processed. To the contrary, Candelore ensures that the scrambling of data does <u>not</u> affect program execution by providing a "*block reordering circuit multiplexer 112. . .which communicates with bus 115 to reverse the re-ordering as necessary for the encryption/decryption circuit 120 and authentication circuit 125 to perform their functions.*"

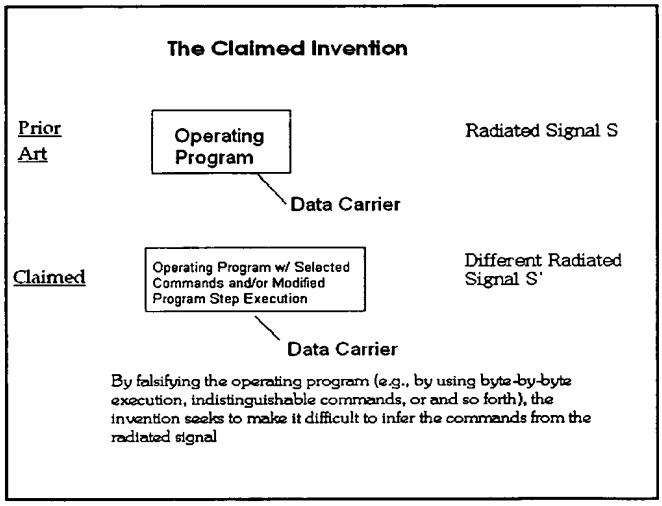
The Candelore patent essentially is concerned with a different problem than the claimed invention. It is concerned with interception of data transmission. It is not concerned with radiation by the processor as it executes the program that requires the data being transmitted from the external memory. Candelore takes no steps to prevent discovery of program execution by detecting radiation generated by the processor. **The radiation generated by a processor as it executes a program is not the same as data being transmitted from an external memory to the processor.** The claimed invention concerns the former while Candelore concerns the latter.

In the Advisory Action, the Examiner states that "*Applicant appears to agree with the Examiner that Candelore does disclose that operations are performed in a manner in which the data being processed cannot be determined from the detected signals that are produced.* In reply, the Applicant respectfully submits that the Examiner has misunderstood the several pages of argument presented in the last response, which attempted to explain that what Candelore discloses is scrambling transmitted data so that the manner in which the data is used cannot be detected, which is not at all the same as the claimed disguising of operations being performed by a processor so that the data used in the operations cannot be discovered by detecting radiation emitted by the processor.

Similarly, it appears that the Examiner has misunderstood the arguments concerning the Dunlavy reference. The Examiner is again urged to refer to the sketches showing the operation

of the claimed invention in comparison with the system disclosed in the Dunlavy patent. In the claimed invention, execution of a program is modified so that the signal radiated by the processor is changed from **S** to **S'**. This is a very simple concept, and yet it is not even close to being suggested in the Dunlavy patent, ***which does <u>not</u> modify the signal S***. Instead, a masking signal is transmitted at the same time as the signal **S. Basically, in Dunlavy, <u>the original signal S is generated by the processor because no attempt is made to change program EXECUTION which results in radiation of the signal S</u>.** ***Adding a signal to S is not the same as modifying program execution to modify S.*** In Dunlavy, S and not S' is generated. The claimed invention specifically recites modification of program execution, or selection of program steps, in order to obtain modified signals S' that will not reveal the data used or processed by the selected program steps.





<u>In summary:</u>

- **The Candelore patent discloses scrambling of data transmissions to and from a processor, but is not concerned with modification of signals radiated by the processor during execution of a program.**

- **The Dunlavy patent discloses generation of a masking signal *instead of* modification of signals radiated by the processor.**
- **Therefore, *neither* reference discloses the claimed modification of signals radiated by the processor during execution of a program by modifying program execution or selection of program steps whose corresponding radiated signals obfuscate the data processed by the steps.**

Accordingly, withdrawal of the rejection of claims 1-4, 13-25, and 34-41 under 35 USC §103(a) is respectfully requested.

3. Rejection of Claims 5-12 and 26-33 Under 35 USC §102(e) in view of the Candelore and Dunlavy Patents, and U.S. Patent No. 6,373,946 (Johnston)

This rejection is again respectfully traversed on the grounds that the Johnston patent, like the Candelore and Dunlavy patents, does not disclose or suggest **execution of commands** in the operating program of a data carrier in such a way that the data processed by the corresponding commands cannot be inferred from signals detectable from outside the semiconductor chip of the data carrier. Instead, the Johnston patent merely relates to encryption of data by a semiconductor chip. There is nothing in the encryption method of Johnston to prevent an attacker from analyzing signals emitted by the chip that does the encryption in order to deduce the program steps used in the encryption and thereby reconstruct the encryption keys based on the deduced program steps and an intercepted output.

The Johnston patent concerns a particular encryption method for securing communications, involving use of a common encryption key, transmittal of the key is a secure memory using the exclusive OR operation to mask the keys. While masking of the keys using the XOR operation is a technique that is also used by the present invention (and in fact is a very basic data masking technique), the key masking is not used in the same way as that of the claimed invention. In Johnston, the keys are masked using exclusive OR, *and then unmasked at the receiving end so that they can be used to decrypt the transmitted communication.* There is no modification of the decryption algorithm to compensate for the masked keys. In the claimed

invention, the masked input data is directly applied to the processing operations carried out by the chip, and the processing operations are varied accordingly so that the **processor performs modified operations on modified input data**. As a result, only the modified input data can be inferred from the signals emitted by the chip during processing.

In the Official Action, the Examiner counters by arguing that modification of a decryption algorithm to compensate for masked keys is not explicitly claimed, and that "*The Examiner believes that Johnston does read on the claimed limitation (recited in Claim 5, for example) that output data is combined with an auxiliary function value to compensate for the falsification of the input data (see Johnston, column 10, lines 38-53).*" This statement evidences a misunderstanding of the above argument, which is simply that there is nothing in the Johnston reference, or either of the other two applied references, to suggest use of Johnston's XOR operation in the manner claimed, which is to effect enable modification of operating program execution so that it is difficult to infer the steps of the operating program based on signals generated by a processor.

The Examiner's statement that Johnston is applicable to the claimed invention because the claimed invention does not recite compensation for masked keys is a ***non-sequitur.*** The point of the Applicant's argument is simply that Johnston teaches key masking steps that have nothing to do with, and could not be used in connection with, what **is** claimed (program execution modification). If the Examiner were to cite a reference disclosing a garden hose, the rejection would not be proper simply because the claim failed to recite that the security processor is *not* a garden hose. Similarly, the fact that Johnston teaches key masking steps that the ordinary artisan would not have associated with the problem of processor emissions (*i.e.*, which involve disguising the **end result** of the process rather than the process itself) is not negated because the claims do not recite the *lack* or *absence* of a key masking step of the type taught in Johnston.

The Johnston patent is not at all concerned with signals emitted by the chip during execution of program steps, but only with the overall results of the execution, *i.e.*, with communications between processors. Therefore, it is respectfully submitted that the Johnston,

Candelore, and Dunlavy patents could not have suggested the claimed modification of program step execution to make it more difficult to infer program step execution by statistical analysis of radiated signals, and therefore withdrawal of the rejection of claims 5-12, and 26-33 under 35 USC §103(a) is respectfully requested.

Having thus overcome each of the rejections made in the Official Action, withdrawal of the rejections and expedited passage of the application to issue is requested.

Respectfully submitted,

BACON & THOMAS, PLLC

By: BENJAMIN E. URCIA
Registration No. 33,805

Date: July 22, 2005

BACON & THOMAS, PLLC
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314

Telephone: (703) 683-0500

NWB:S:\Producer\beu\Pending Q...Z\V\VATER 700656\a03.wpd